16869N-0439 ~~0342~~

JC979 U.S. PTO
10/081551
02/20/02

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２００１年１２月１１日

出 願 番 号
Application Number: 特願２００１－３７６５７５

[ST.10/C]: [ＪＰ２００１－３７６５７５]

出 願 人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００２年 １月２５日

特 許 庁 長 官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　KO1012541A
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション事業部内
【氏名】　青島　達人
【発明者】
【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション事業部内
【氏名】　田坂　光伸
【発明者】
【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション事業部内
【氏名】　武田　景
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　ログイン認証方法およびその実施システム並びにその処理プログラム

【特許請求の範囲】

【請求項１】

業務システムおよび商用サービスシステムを利用するユーザのログイン認証方法において、

前記業務システムにログインしているユーザが前記商用サービスシステムを利用するときに、ユーザの使用しているクライアントから前記業務システムに前記商用サービスシステムの利用要求を送信し、

利用要求を受信した前記業務システムはユーザの商用サービス利用権限をチェックし、認証に先立ち作成したパスワードリストからパスワードを１つ選択して前記クライアントへ返し、

前記クライアントは返されたパスワードを前記商用サービスシステムに送信し、

前記商用サービスシステムでは認証に先立ち作成したアカウント情報との比較を行い、一致しているときはログインを許可し、前記使用したパスワードを無効化することを特徴とするログイン認証方法。

【請求項２】

請求項１のログイン認証方法において、

前記パスワードリストを前記業務システムが乱数を用いて生成し、前記商用サービスシステムに前記パスワードリストを送信しアカウント情報を作成することを特徴とするログイン認証方法。

【請求項３】

請求項１において、

前記アカウント情報を前記商用サービスシステムが乱数を用いて生成し、前記業務システムに前記アカウント情報を送信し前記パスワードリストを作成することを特徴とするログイン認証方法。

【請求項４】

請求項１のログイン認証方法において、

前記パスワードリストを前記業務システムが任意の数値と一方向性関数を順次適用した値を用いて生成し、前記商用サービスシステムに前記一方向性関数の適用回数と順次適用した最終結果の数値を送信して前記アカウント情報を作成し、

前記クライアントからの商用サービスシステム利用要求時に、前記業務システムが前記クライアントにパスワードと前記一方向性関数の適用回数を返し、前記商用サービスシステムでのログイン許可判定時に、前記クライアントから送信されたパスワードに前記一方向性関数を前記最終結果の適用回数から前記パスワードに対する前記一方向性関数の適用回数を引いた分だけ適用した結果と前記アカウント情報内の前記最終結果の数値との比較を行い、一致していればログインを許可することを特徴とするログイン認証方法。

【請求項５】

請求項４のログイン認証方法において、

前記商用サービスシステムでのログイン許可判定時に、順次適用した結果の数値を保存しておき、判定するパスワードの前記一方向性関数の適用回数から保存した結果の前記一方向性関数の適用回数を引いた回数分だけ保存した結果に適用することを特徴とするログイン認証方法。

【請求項６】

業務システム、商用サービスシステムおよびクライアントを有する計算機システムにおいて、

前記業務システムにログインしているユーザが前記商用サービスシステムを利用するときに、前記業務システムに前記商用サービスシステムの利用要求を送信するクライアントと、

利用要求を受信し、前記ユーザの商用サービス利用権限をチェックし、認証に先立ち作成したパスワードリストからパスワードを１つ選択して前記クライアントへ返す業務システムとを備え、

前記クライアントは、返されたパスワードを前記商用サービスシステムに送信し、

前記商用サービスシステムは、認証に先立ち作成したアカウント情報との比較

を行い、一致しているときはログインを許可し、前記使用したパスワードを無効化することを特徴とする計算機システム。

【請求項７】

請求項６記載の計算機システムにおいて、

前記業務システムは、前記パスワードリストを乱数を用いて生成し、前記商用サービスシステムに前記パスワードリストを送信しアカウント情報を作成する手段を備えたことを特徴とする計算機システム。

【請求項８】

請求項６記載の計算機システムにおいて、

前記商用サービスシステムは、前記アカウント情報を乱数を用いて生成し、前記業務システムに前記アカウント情報を送信し前記パスワードリストを作成する手段を備えたことを特徴とする計算機システム。

【請求項９】

請求項６記載の計算機システムにおいて、

前記業務システムは、前記パスワードリストを任意の数値と一方向性関数を順次適用した値を用いて生成し、前記商用サービスシステムに前記一方向性関数の適用回数と順次適用した最終結果の数値を送信して前記アカウント情報を作成する手段と、前記クライアントからの商用サービスシステム利用要求時に、前記クライアントにパスワードと前記一方向性関数の適用回数を返し、前記商用サービスシステムでのログイン許可判定時に、前記クライアントから送信されたパスワードに前記一方向性関数を前記最終結果の適用回数から前記パスワードに対する前記一方向性関数の適用回数を引いた分だけ適用した結果と前記アカウント情報内の前記最終結果の数値との比較を行い、一致していればログインを許可する手段を備えたことを特徴とする計算機システム。

【請求項１０】

請求項９記載の計算機システムにおいて、

前記商用サービスシステムは、ログイン許可判定時に、順次適用した結果の数値を保存しておき、判定するパスワードの前記一方向性関数の適用回数から保存した結果の前記一方向性関数の適用回数を引いた回数分だけ保存した結果に適用

する手段を備えたことを特徴とする計算機システム。

【請求項１１】

業務システムおよび商用サービスシステムを利用するユーザのログイン認証プログラムにおいて、

前記業務システムにログインしているユーザが前記商用サービスシステムを利用するときに、ユーザの使用している上記クライアントから前記業務システムに前記商用サービスシステムの利用要求を送信するステップと、

利用要求を受信した前記業務システムはユーザの商用サービス利用権限をチェックし、認証に先立ち作成したパスワードリストからパスワードを１つ選択して前記クライアントへ返すステップと、

前記クライアントは返されたパスワードを前記商用サービスシステムに送信するステップと、

前記商用サービスシステムでは認証に先立ち作成したアカウント情報との比較を行い、一致しているときはログインを許可し、前記使用したパスワードを無効化するステップとを有することを特徴とするログイン認証プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

業務システムを利用しているユーザに商用サービスシステムを安全に利用させ、業務システムを使用している複数ユーザが商用サービスシステムのアカウントを共有可能なログイン認証技術に関する。

【０００２】

【従来の技術】

現在、ユーザがイントラネットの業務システムとインターネットを介した様々な商用サービスを同時に利用することも多い。イントラネットの業務システムはユーザの職務権限に応じた処理を可能とするためにログイン認証を行うが、前記のインターネットを介したサービスに関しても、有料であればサービス利用時にログイン認証が必要になる。このような複数システムの利用には以下の要件がある。

（１）商用サービスシステムを社内から利用させる場合、ユーザに、利用しているシステム／サービスを意識させない。すなわち商用サービスシステムのログイン認証を明示的に行わせない。

（２）商用サービスシステムを利用できる社内ユーザを職務権限に応じて限定したいため、ログイン認証に関する情報（アカウント）についてのセキュリティにも配慮する必要がある。すなわち、パスワードが他ユーザに漏れた場合でもログイン認証で拒否する。

（３）既に稼動している業務システムと商用サービスを連携させる場合もあるため、業務システムへの負荷を最小限に抑える。

（４）商用サービスを利用するアカウントを企業内のユーザ分確保することは課金等の面で現実的でない場合が多いため、複数の企業内ユーザがアカウントを共有することができる。

【０００３】

（１）の要件を満たすために、クライアントから商用サービスを直接利用できるように、業務システムとサービスシステムとの間で取り決めたプロトコルに従って生成した特別なキーをクライアントに渡す方法が考えられる。この場合、（２）の要件を満たすためには、キーに通常のログイン認証における固定的なユーザIDとパスワードは利用できない。上記のログイン認証機能を実現するために、所謂ワンタイムパスワードの利用が考えられる。ワンタイムパスワードの原型は、Lamport's Hashアルゴリズムであり、Leslie Lamport, Password Authentication with Insecure Communication, Communications of the ACM 24, 11 (November 1981), 770-772.に記載されている。

【０００４】

【発明が解決しようとする課題】

Lamport's Hashアルゴリズムでは、どこまでパスワードを消費したかを表す数nを問合せることにより次に利用するパスワードを決定し、サービスシステム側には、このnおよび対応するハッシュ値のみ記憶しておけばよい。ただし、このワンタイムパスワードを前記の業務システムと商用サービスシステムに適用するには以下の２つの課題がある。

【０００５】

１つめは、業務システムとサービスシステムとの間でLamport's Hashアルゴリズムに従った通信を行うため、業務システムとサービスシステムとの間で複数回の通信を行う必要がり、業務システムの負荷が高くなることである。

【０００６】

２つめは、サービス側で保存しているのは１つのハッシュ値だけであり、１つのアカウントを複数人で同時に利用できないことである。

【０００７】

本発明の目的は、通信量を減らし、１つのアカウントの複数人での並行利用を可能にするログイン認証方法およびその実施システムを提供することである。

【０００８】

【課題を解決するための手段】

本発明の特許請求の範囲第１項に記載された方法では、現在どこまでパスワードを利用したかを問合せする通信を行わずに済むため、通信量を減らすことができる。また特許請求の範囲第２項または第３項に記載された方法により、商用サービスシステムには予め全てのパスワードが送信されているため、複数人で同時にログイン処理を行うことができる。

【０００９】

【発明の実施の形態】

以下、本発明の一実施の形態を説明する。

【００１０】

図１は、本発明の一実施例における処理方法の全体図を示したものである。企業内には業務システム１とユーザが利用するクライアント３（端末または計算機）がある。ユーザは業務システム１に対してログインしているものとする。また、ユーザは外部の商用サービスサイトに存在するサービスシステムも利用する。商用サービスシステムでは、利用者を管理するためアカウント情報４１を利用者ごとに持っている。このアカウント情報４１を複数のユーザが共有して利用する場合を考える。

【００１１】

ログイン認証に先立って、業務システム内でパスワードリスト４０を生成する。このパスワードリスト４０内にはN個のパスワードがある。ここでは、個々のパスワードを乱数から生成するものとする。このパスワードリスト４０をサービスシステム２に送信５００して、アカウント情報４１内のパスワードに格納しておく。また各パスワードには、このパスワードが使用済みか未使用かを表すフラグを組にして格納しておく。このフラグの初期値は未使用である。

ユーザが商用サービスを利用する場合には、ユーザの使用しているクライアント３から業務システム１に商用サービスシステム２の利用要求を送信５０１する。利用要求を受信した業務システム１はユーザの商用サービス利用権限をチェック５０２し、利用権限があるなら前記パスワードリスト４０から任意のパスワード４０１を１つ選択５０３してクライアントに返す５０４。

【００１２】

クライアント３は返されたパスワードを商用サービスシステム２に送信５０５する。

商用サービスシステム２では、アカウント情報４１内のパスワードとの比較５０６を行い、一致するパスワード（この場合４１１）が存在すればログインを許可する。また、商用サービスシステム２は使用したパスワードを無効化５０７するために、使用したパスワードと組になっているフラグを使用済みに変更する。

【００１３】

上記の一連の処理において、各ユーザに必ず異なったパスワードを割り当てることにより、１つのアカウントに対して複数ユーザで同時にログイン認証処理を行うことができる。

以上が一実施の形態の説明であるが、この実施例の変形例として、ワンタイムパスワードのアルゴリズムを修正して本発明の処理方法に適用した場合の実施例を以下に説明する。

【００１４】

図２のパスワードリストを用い、第１の実施例におけるパスワードリスト４０を置き換えた第２の実施例について説明する。ここでは、個々のパスワードを任意の初期値rに対してハッシュ関数を順次適用して生成する。ここで、Hash[n](r

)４０２はrに対してハッシュ関数をn回適用した結果を表す（４０２）。

【００１５】

ログイン認証に先立って、業務システムはハッシュ関数の総適用回数N およびHash[N](r)のみをサービスシステム２に送信５００しておく。

【００１６】

図３のアカウント情報を用い、第１の実施例におけるアカウント情報４１を置き換えた第３の実施例について説明する。ここで各パスワードには、このパスワードを計算したときのハッシュ関数の適用回数、および、このパスワードが使用済みか未使用かを表すフラグを組にして格納しておく（４１２）。初期段階では、アカウント情報には、Hash[N](r)とNと未使用の組だけを格納する。

【００１７】

ユーザからの商用サービス利用要求を受信したときの、業務システム１のパスワード選択処理５０３は、適用回数nの大きなパスワードから順に割り当てることになる。

【００１８】

クライアントへの返信処理５０４では、パスワード４０２と共に適用回数nも返す。

商用サービスシステム２での比較処理５０６では、クライアントから送信されたパスワードHash[n](r)にHash関数を総適用回数Nから適用回数nを引いた分だけ適用した結果（Hash[N-n](パスワード)）とHash[N](r)の数値とを比較し、一致すればログインを許可する。

【００１９】

さらに、商用サービスシステム２でのハッシュ関数の計算量を減らすための例を示す。

商用サービスシステム２での比較処理５０６では、ハッシュ関数を適用する計算を複数回行うため、それぞれの中間結果をアカウント情報４１に追加していく。ここで、適用回数がmまで計算が行われている場合、ハッシュ関数の計算はHash[m-n](パスワード)となり、結果をHash[m](r)と比較する。このとき、適用回数nからmまでの中間結果を保存することになり、これ以降、nより大きくmより小さ

い適用回数のパスワードの比較処理においては、ハッシュ関数の計算を行わない。

【００２０】

以上により、利用しているシステム／サービスをユーザに意識させずに、業務システムと商用サービスシステムを利用させることができる。

また、「特定のユーザしか商用サービスを利用できない」という業務上の制限を安全に満たすことができる。

また、業務システムと商用サービスシステム間の通信量を削減することができる。

また、商用サービスシステムの１つのアカウントを複数人で共有利用することができる。

【００２１】

【発明の効果】

本発明によれば、通信量を減らし、１つのアカウントの複数人での並行利用を可能にする

【図面の簡単な説明】

【図１】本発明の一実施例における処理方法の全体図

【図２】本発明のパスワードリストの構成図である。

【図３】本発明のアカウント情報おける処理方法の全体図

【符号の説明】

１　業務システム

２　商用サービスシステム

３　クライアント

４０　パスワードリスト

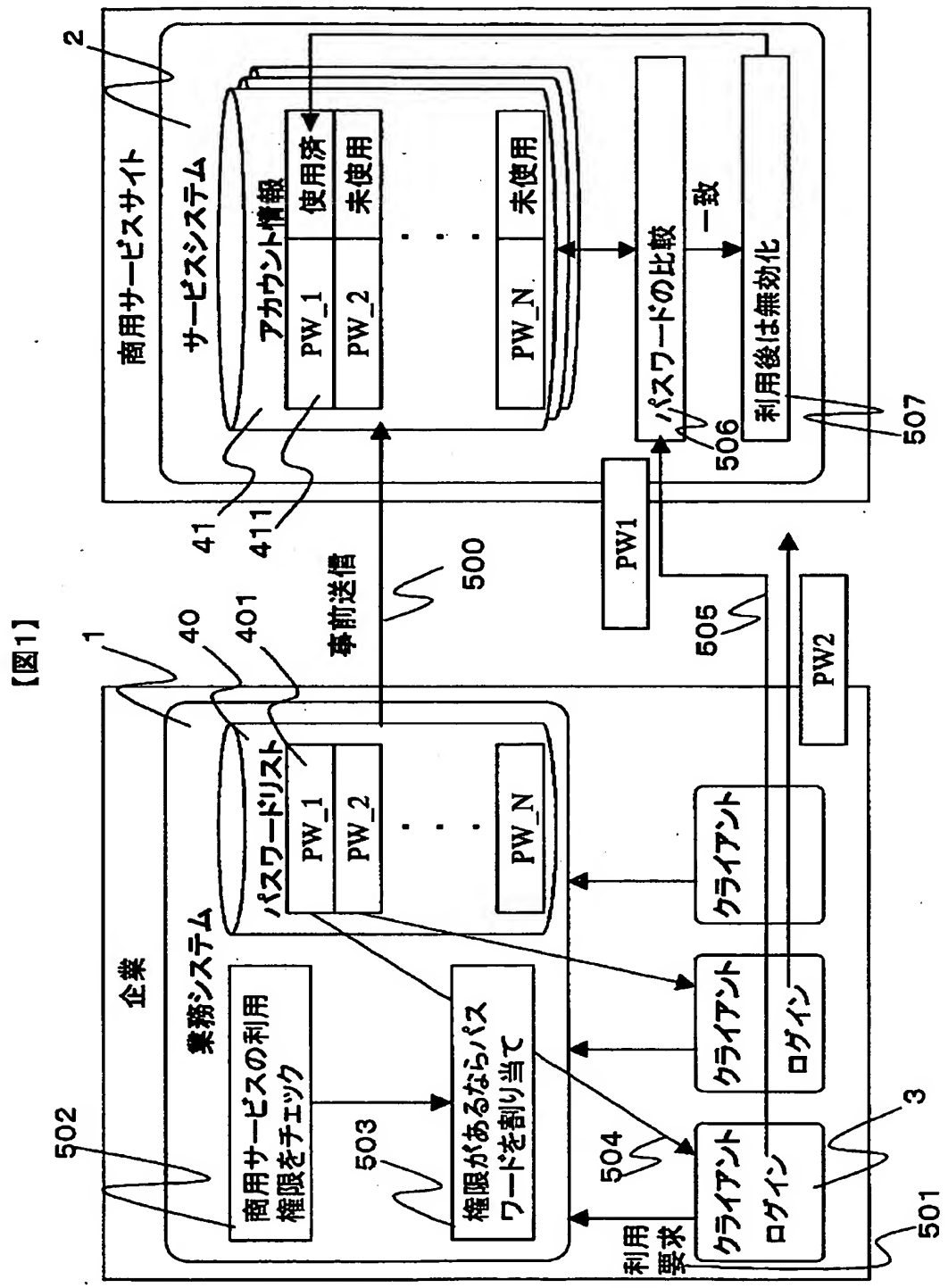
４０１　パスワード

４１　アカウント情報

４１１　パスワードと使用済み／未使用フラグとの組

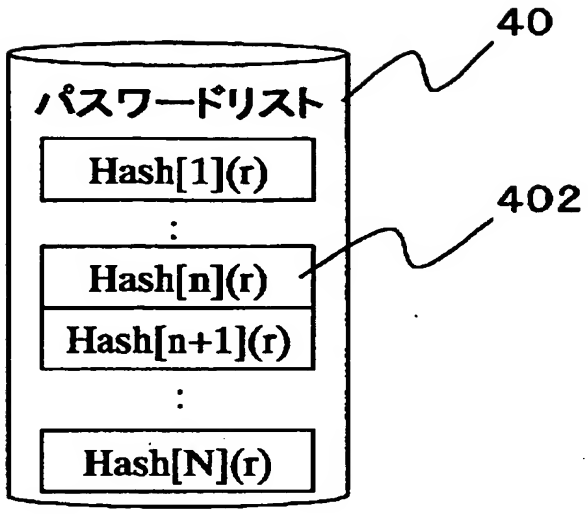
【書類名】　図面

【図１】


【図1】
1
2
40
401
41
411
500
505
506
507
502
503
504
501
3
商用サービスサイト
サービスシステム
アカウント情報
使用済
未使用
PW_1
PW_2
PW_N
パスワードの比較
一致
利用後は無効化
PW1
PW2
事前送信
企業
業務システム
パスワードリスト
商用サービスの利用権限をチェック
権限があるならパスワードを割り当て
クライアント
ログイン
利用要求

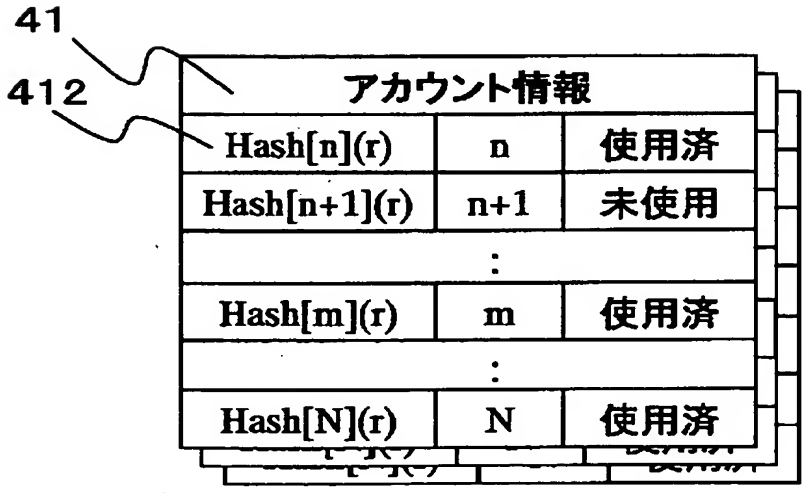
【図２】

【図2】


40
パスワードリスト
Hash[1](r)
402
Hash[n](r)
Hash[n+1](r)
Hash[N](r)

【図３】

【図3】


41
412
アカウント情報
Hash[n](r)
n
使用済
Hash[n+1](r)
n+1
未使用
Hash[m](r)
m
使用済
Hash[N](r)
N
使用済

【書類名】　要約書

【要約】

【課題】

業務システムおよび商用サービスシステムを利用するユーザのログイン認証方法において、通信量を減らし、１つのアカウントの複数人での同時利用を可能にすることである。

【解決手段】

認証に先立ち業務システムがパスワードリストを生成し、商用サービスシステムに前記リストを送信しておく。ユーザの使用しているクライアントから業務システムに商用サービスシステム２の利用要求を送信すると、利用要求を受信した業務システムはユーザの商用サービス利用権限をチェックし、前記パスワードリストからパスワードを１つ選択してクライアントに返す。クライアントは返されたパスワードを商用サービスシステムに送信し、商用サービスシステムでは、アカウント情報（パスワードリスト）内のパスワードとの比較を行い、一致していればログインを許可し、使用したパスワードを無効化する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００１－３７６５７５
受付番号	５０１０１８１２７６３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１３年１２月１２日

＜認定情報・付加情報＞

【提出日】　平成13年12月11日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所